

# VOIP Corp. Procedures for Disclosure of CPNI

VoIP Corp is committed to maintaining the privacy of its customers and protecting their CPNI and other all other customer data. The procedures we follow are set out below.

## **WHAT IS PROTECTED**

VoIP Corp has a duty, under federal law, to protect the confidentiality of certain types of customer proprietary network information (CPNI), including: (1) information about the quantity, technical configuration, type, destination, location, and amount of use of a Customer's services, and (2) information contained on the service bill concerning services a Customer receives. CPNI includes information typically available from the telephone-related details on a monthly bill, such as technical information, type of service, current charges, long distance and local service billing records, directory assistance charges, usage data and calling patterns.

## **HOW IT IS PROTECTED**

VoIP Corp does not use third party marketing organizations.

VoIP Corp's protection of CPNI begins with training. All our employees and staff members are trained on how CPNI is to be protected and when it may or may not be disclosed. Violation of this CPNI policy by any employee will result in disciplinary action against that employee, as set forth in VoIP Corp's Employee Manual.

VOIP Corp has different procedures in place depending on the method by which a party seeks access to CPNI.

### **Initial Verification**

VoIP Corp authenticates each customer's identity and requires him or her to select a password upon service initiation. We do not use readily available personal information or account information in setting up the procedure for subsequent authentication for purposes of making account changes or allowing the customer access to CPNI related to his or her account. Once the customer's identity is initially authenticated, the customer may only obtain access to his or her CPNI online, through use of a password.

### **No Telephone Access to CPNI**

VoIP Corp has a strict policy and will not release CPNI over the telephone during customer-initiated telephone contact.

### **Internet Access**

To get access to information such as call detail records and other customer proprietary

information, all customers must log into their account over the Internet. They must use their telephone number of record and their designated password.

### **Lost or Forgotten Passwords**

In the event a customer has lost or forgotten a password, he or she must contact VOIP Corp. and we use the information selected at account initiation – which is neither readily available personal information nor account information – to verify the caller’s identity and request. Only then is the account password sent to the caller via email. The email address used is the one already on record, which was obtained from the customer upon service initiation.

### **Notification of Account Changes**

VoIP Corp notifies its customers immediately whenever there is CPNI-related account activity, such as a password change, a customer inquiring for a lost or forgotten password, the creation of a new online account, or the change of the address of record. The first notification, including the selection of a password at service initiation, is sent to the customer upon activation of service. Subsequent notifications are sent to the customer at the then-current email address of record, and do not reveal the changed information.

### **Business and Wholesale Customers**

In dealing with business and wholesale customers, VOIP Corp. ordinarily contracts for authentication regimes other than those described in Sections 64.2010 and 64.2011 of the FCC rules because it provides those customers with a dedicated account representative and it enters into a contract that specifically addresses its and the customer’s protection of CPNI.

## **BREACH OF CPNI PRIVACY**

In the event VoIP Corp experiences a privacy breach and CPNI is disclosed to unauthorized persons, federal rules require VoIP Corp to report such breaches to the U.S. Secret Service and the FBI. Any VoIP Corp employee learning of such a breach must notify senior management immediately. VOIP Corp. will notify law enforcement no later than seven (7) business days after it has reasonably determined that such breach has occurred by sending electronic notification to the United States Secret Service and the FBI through the central reporting facility at [www.fcc.gov/eb/cpni](http://www.fcc.gov/eb/cpni).

No employee shall notify any customer of a breach without written authorization from the CEO of VoIP Corp. By law, VOIP Corp cannot inform its customers of the CPNI breach until at least seven (7) days after notification has been sent to law enforcement, or later if the law enforcement agency tells it to postpone disclosure pending investigation.

VoIP Corp is required to and will maintain records of any discovered CPNI breaches, the date that it discovered the breach, the date it notified law enforcement and copies of the notifications to law enforcement, a detailed description of the breach, including the circumstances of the breach, and law enforcement's response (if any) to the reported breach. VoIP Corp will retain these records for a period of not less than two (2) years.

#### **NOTIFICATION OF CHANGES TO THIS POLICY**

If we change this CPNI Policy, we will post those changes to our website or in other places we deem appropriate, so that our customers can be aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it.